城市网络信息安全建设的影响因素与组态路径研究

——基于 36 个重点城市的模糊集定性比较分析

吴钟灿[1]　郝文强[2]

[1]中央民族大学管理学院　北京 100081　[2]复旦大学国际关系与公共事务学院　上海 200433

摘　要：[目的/意义]网络信息安全攸关个人利益、社会稳定乃至国家安全，如何提高网络信息安全水平成为亟需解决的重要议题。[方法/过程]本文基于 TOE 理论，运用模糊集定性比较分析法，从技术、组织、环境三个方面对我国网络信息安全建设的影响因素与组态路径进行分析。[结果/结论]研究发现，技术、组织与环境多种因素耦合，形成了机构-经济依赖型、制度-环境联动型、领导-经济激励型、机构-人才支持型 4 种高水平的城市网络信息安全建设路径。此外，不同地域的城市网络信息安全建设呈现差异化路径，东部城市主要通过领导推动、制度推动、领导与经济联动实现高水平的网络信息安全建设，中西部城市主要通过制度与技术联动、制度与经济联动实现高水平网络信息安全建设。研究结论为城市网络信息安全建设提供了多元路径解释，对于因地制宜地推动城市网络信息安全建设具有重要启示。

关键词：城市网络信息安全　技术驱动　组织支持　环境依赖　模糊定性比较分析

1　引言

中共二十大提出“必须坚定不移贯彻总体国家安全观，把维护国家安全贯穿党和国家工作各方面全过程”。网络信息安全是国家安全的重要组成部分，尤其是在大数据时代，网络空间越来越成为国家安全战略的必争之地[1]。我国高度重视网络信息安全工作，2014 年，中央网络信息安全与信息化领导小组成立，标志着网络信息安全正式上升为国家层面的重点议题[2]。2016 年，中共中央网络安全和信息化委员会办公室发布《中华人民共和国网络信息安全法》，要求“保障网络信息安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和

*本文系教育部哲学社会科学重大课题攻关项目“新时代特大城市管理创新机制研究”（项目编号：20JZD030）研究成果之一。
作者简介：吴钟灿（ORCID:0000-0002-5595-3795），博士研究生；郝文强（ORCID:0000-0002-1856-9647），博士研究生，通讯作者，Email:1136979001@qq.com.

其他组织的合法权益，促进经济社会信息化健康发展”[3]，这是我国第一部全国性网络信息安全法，也昭示着网络信息安全已经被纳入国家法律保护范围。

网络信息安全对于城市安全尤为重要，城市作为行政区划中网络信息安全的重要防线，是抵御网络风险的重要关卡。在国家智慧城市建设的倡议下，网络信息安全已经成为建设智慧城市的战略重点[4]。然而，现阶段我国各城市之间网络信息安全水平存在较大差异，是何种原因造成了各城市间网络信息安全水平的差异？城市网络信息安全建设存在哪些不同路径水平？各因素之间又存在何种联动关系？这些都是当前网络信息安全建设亟需研究的重要问题。

2 文献综述

网络信息安全是指在保障网络系统硬件、软件正常运行的前提下，保障网络系统中的数据在存储和传输过程中不受侵害而遭到破坏。网络信息安全具有信息的完整性、一定范围内的保密性、信息的可用性和可控性、抗抵赖性等特征[5]。作为全球网络技术领先者和互联网的缔造者，美国是最早关注网络信息安全防护的国家[6]。20 世纪 70 年代以来，随着信息技术不断发展和进步，越来越多的网络信息安全问题引起了国内外学者的广泛关注[7]。已有研究在网络信息安全的影响因素与实现路径等方面取得了实质性的进展[8]。

关于网络信息安全的影响因素，主要形成了技术决定论、组织影响论和环境制约论三种观点。技术决定论认为，网络信息安全主要受到技术因素的影响。学者们分别揭示了网络信息安全的技术设备[9]、软件设计[10]、信息技术发展[11]、信息技术和信息心理[12]、防护墙技术[13]等方面的漏洞，发现当前网络信息安全的技术尚未成熟，难以积累相关的网络信息安全知识[14]，影响了网络信息安全建设进程。组织影响论认为，网络信息安全主要受到组织结构因素的制约。研究发现，网络信息安全的人员管理[15]、部门管理[16]、工作人员的防护技能[17]、网络信息安全监管法治化水平[18]等诸多因素都会对网络信息安全产生的影响。环境制约论强调网络信息安全主要受到环境因素的制约，包括网络信息安全责任主体、安全边界、安全焦点[19]、公众的受教育程度[20]、网络信息安全主体的信息保护意识[21]、用户信息安全意识和安全防范能力[22]等。

围绕网络信息安全建设的实现路径，学者们进行了广泛讨论，主要形成了一

下观点。一是提高主体的网络信息安全意识。如 S.A.Fadhil[23]、A.Ghadge[24]等学者认为现代信息通讯技术给网络信息安全带来了挑战，因此提高主体的网络信息安全意识可以有效应对网络信息安全风险。二是建立网络信息安全模型。例如，T.Kawanak 等[25]、J.Chen 等[26]分别提出网络信息安全外部信息泄露模型和网络信息安全信息系统评价体系模型，为网络信息安全提供了良好的应对措施。三是加强网络信息安全制度建设。马晓飞等[27]、马民虎等[28]通过研究国外发达国家的网络信息安全制度实践，指出我国应该通过完善网络信息安全信息制度建设来加强国内网络信息安全建设。

综上所述，学界较为系统地回答了网络信息安全受到哪些因素的制约，为本文研究问题的破解提供了思路，但仍存在以下不足有待拓展：首先，既有研究大多是对网络信息安全问题的规范性分析，缺乏对网络信息安全影响因素的实证检验。本文拟从技术、组织、环境三个维度出发，对影响网络信息安全的诸多因素进行系统识别与检验。其次，既有研究多关注单个因素对网络信息安全的线性影响，相对忽视了技术、组织和环境等多元因素对网络信息安全的共同作用。本文拟运用模糊集定性比较分析方法，对影响网络信息安全的多因素组合作用进行深入分析，揭示城市网络信息安全建设的多元路径。最后，目前关于网络信息安全的研究多聚焦于国家层面的宏观分析，鲜有学者关注城市层面网络信息安全水平的差异及其影响因素。基于此，本文从 TOE 理论框架出发，以 36 个重点城市作为样本，探讨影响城市网络信息安全建设的组态路径，以期为我国不同地方政府提高网络信息安全水平提供指导。

3 理论基础与研究框架

TOE（Technology-Organization-Environment）理论框架源于 20 世纪 90 年代，最早由 L.G.Tornatzky 等[29]在《技术创新的流程》中提出。TOE 理论被广泛应用于分析企业采纳创新技术的影响因素，后来逐渐发展成为一种基于技术应用情境的综合性分析框架[30]。该理论认为，组织采纳创新技术受到技术、组织和环境三个方面因素的共同影响。技术因素是指技术的相关特性，包括技术能力、技术资源等；组织因素是指组织本身的特征，包括组织的层级、规模、结构等；环境因素是指组织受到的外部因素的影响，包括经济发展、需求压力等。

目前，TOE 理论已广泛应用于电子政务、政府开放数据研究等议题研究中。在我国地方政府网络信息安全实践中，各城市网络信息安全水平呈现较大差异，反映了网络信息安全的影响因素复杂多样，其中蕴含着多重驱动机制。基于此，对网络信息安全水平背后反映出的技术、组织、环境等多重条件的组态分析便具有十分重要的现实意义。本文从 TOE 框架的理论视角出发，将影响我国城市网络信息安全水平的因素划分为技术、组织、环境三方面（见图 1）。其中，技术因素包括网络信息安全人才、网络信息安全技术两个影响因素。组织因素包括主要领导重视、安全管理制度、安全机构设置三个影响因素。环境因素包括经济条件支持、社会需求压力两个因素。技术、组织、环境三者之间相互联动、共同作用于数字城市网络信息安全指数。

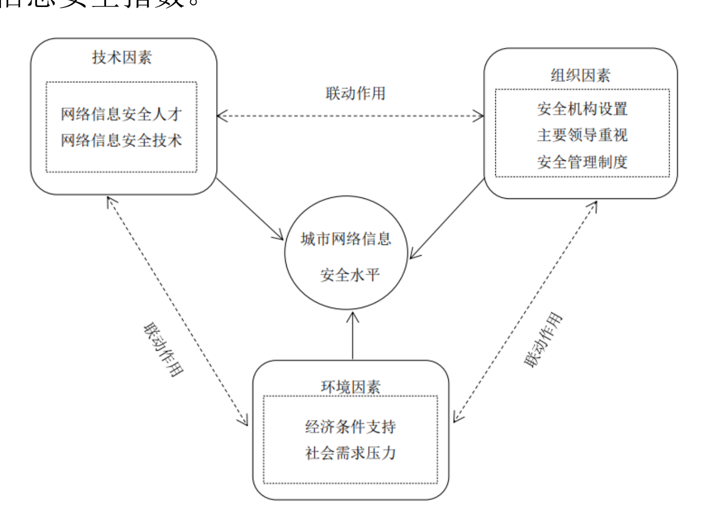


图 1　城市网络信息安全水平分析框架

3.1　技术因素

技术因素是指影响网络信息安全的技术特征及其与组织的关系，主要涵盖了网络信息安全人才和网络信息安全技术两个方面。一方面，人才是网络信息安全体系建设的重要保障[31]。作为一项技术性活动，网络信息安全的功能设计、体系运维等都依靠网络信息安全人才实现。网络信息安全人才数量的多少、水平与质量的高低，影响着一个地方政府的网络信息安全水平。另一方面，网络信息安全技术是维护网络信息安全的关键工具，是网络信息安全的重要保障[32]。网络作为虚拟事物，需要通过网络信息安全技术来支持网络平台的平稳运行、系统维护、功能开发、风险阻截等。

3.2 组织因素

从组织因素出发，影响城市网络信息安全的因素包括主要领导重视、安全机构设置、安全管理制度。首先，主要领导对网络信息安全的重视程度决定了网络信息安全建设的力度，从而影响其对网络信息安全的资源投入和网络信息安全的考核比重。政府主要领导人对网络信息安全的重视为网络信息安全管理提供了重要的政治保证，是推动网络信息安全政策有效执行的重要法宝。其次，网络信息安全机构在安全测评、系统监测、后台运维等方面为城市网络信息安全建设提供了组织保障，映射了组织网络信息安全的管理能力。网络信息安全组织机构设置越完善，网络信息安全的组织化水平越高。最后，网络信息安全制度为把握网络信息安全风险的发生规律和动向以及突发网络信息安全事件应急处置提供了保障[33]，同时为用户和运维人员使用、维护信息系统提供了指南。网络信息安全制度水平的高低，决定了网络信息安全的法治化水平。

3.3 环境因素

环境因素包括组织所面临的内外部环境。影响城市网络信息安全的环境因素包括政府的经济条件支持和社会需求压力。经济条件支持反映的是城市对网络信息安全管理的资金支持力度。就城市网络信息安全议题而言，城市政府对网络信息安全建设资金投入的多少，决定了政府对城市网络信息安全的基础设施建设、网络信息安全人才的培养等方面是否有足够的资金保障。在社会需求压力方面，既有研究表明，随着我国居民受教育程度的增加，公民的网络信息安全需求与日俱增，对城市网络信息安全建设提出了更高要求[34]。受教育程度越高的公民的网络信息安全意识越强，在个人信息安全受到侵犯，或在网络中遭遇攻击时，越倾向于用法律武器维护自己的权利，从而给城市网络信息安全建设形成自下而上的压力，推动政府网络信息安全建设水平的提升。

4 研究设计

4.1 研究方法

本文采用模糊集定性比较分析(fsQCA)方法进行组态分析。模糊集定性比较分析方法由 C.C.Ragin 在 1987 年提出[35]，是通过分析案例中的多个因果条件，

识别导致被解释变量产生变化的不同因果路径的研究方法[36]。也就是说，模糊集定性比较方法是通过案例本身来挖掘造成同一结果变量产生变化的不同条件，是对“多因一果”进行分析的方法。本研究选择采用模糊集定性比较分析(fsQCA)方法来对网络信息安全的影响因素进行分析，原因有二：一是网络信息安全受到多种因素的影响，传统的回归方法难以对这种复杂的关联现象做出合理的解释；二是模糊集定性比较分析(fsQCA)方法适合分析具有程度或者水平上变化的变量，本文的变量如网络信息安全人才、网络信息安全技术、网络信息安全机构设置等都只是涉及数量和程度的变化，不存在“非此即彼”的类型，因此，相较于清晰集定性(csQCA)比较分析而言，更适合运用模糊集定性比较分析方法进行分析。

4.2 案例选择

本文选择我国 36 个重点城市作为样本，包括 4 个直辖市、27 个省会城市和 5 个计划单列市。首先，城市政府网络信息安全水平具有承上启下的重要作用，既能链接上级政府的网络信息安全要求，也能给基层政府提供相应的指导，因此研究城市政府的网络信息安全水平对推进国家信息化安全建设具有非常重要的价值。其次，36 个城市覆盖了东、中西部不同区域，能够代表不同地区的网络信息安全建设水平，而且这些城市之间在组织、技术和面临的环境方面存在着较大差异，具有较好的代表性和可比性。最后，样本量适当且资料便于获取。本文的样本量为 36 个，符合 QCA 方法 15-50 之间的中等样本量需求，相关数据资料可通过公开网站获取。

4.3 变量设定及其赋值

4.3.1 结果变量

本文要解释的结果变量为数字城市网络信息安全水平，数据来源于 2022 年 6 月由中国电子信息产业发展研究院发布的《数字城市网络安全评估指数白皮书（2022)》。该报告从数字城市网络安全管理体系、数字城市网络安全技术体系和数字城市网络安全运营体系三个方面 11 项指标出发，对数字城市网络信息安全整体状况进行了评估。中国电子信息产业发展研究院作为工业和信息化部直属单位，长期致力于为我国数字化建设提供决策咨询，是我国互联网安全领域的权威

咨询机构，其数据来源具有较高的可信度和权威性。

4.3.2 条件变量

根据相关文献梳理和理论框架的结合，本文按照研究对象的实际情况，将解释变量分为技术、组织、环境三个维度（见表 1）。

表 1 城市高网络信息安全水平变量的设定与校准

变量		变量名称	变量测量	变量校准	数据来源
结果变量		数字城市网络信息安全水平	数字城市网络安全指数	排名前 18 赋值为 1，排名后 18 则赋值为 0	《城市数字化网络信息安全评价指数白皮书 2022》
条件变量	组织维度	安全机构设置	各市网络信息安全等级保护机构数量	三个锚点分别为 75 分位值，50 分位值，25 分为值	2021《全国网络信息安全等级保护测评机构推荐目录》
		主要领导重视	主要领导关于网络信息安全讲话的次数		各省人民政府网站及搜索资料
		安全管理制度	各市出台的网络信息安全制度数	有网络信息安全制度赋值为 1，无网络信息安全制度则赋值为 0	北大法宝
	技术维度	网络信息安全人才	各市计算机软件服务人数	三个锚点分别为 75 分位值，50 分位值，25 分为值	2021《中国城市统计年鉴》
		网络信息安全技术	城市网络信息安全综合指数		《大数据城市网络信息安全指数报告》
	环境维度	经济条件支持	各市政府一般公共预算支出		2021《中国城市统计年鉴》
		社会需求压力	各市在读大学生数		2021 年各市统计年鉴

①网络信息安全人才。网络信息安全人才是网络信息安全建设的主力军，网络平台的功能设计、系统运维等离不开网络信息安全人才队伍的支持。一个城市网络信息安全人才队伍的建设水平，影响着城市网络信息安全的建设水平。计算机软件服务人员是经过网络信息安全培训的技术性人才，其数量是衡量网络信息安全人才的重要指标。各市计算机软件服务人数反映了城市网络信息安全人才队伍建设情况。因此，选取计算机软件服务人数来测量网络信息安全人才，数据来源于 2021 年《中国城市统计年鉴》。

②网络信息安全技术。本文通过大数据协同安全技术国家工程实验室、提升政府治理能力大数据应用技术国家工程实验室和中国赛宝实验室等多个机构联

合发布的《大数据网络信息安全指数报告》（下文简称<报告>）来测量城市网络信息安全水平。该<报告>从政府网络信息安全指数、企业网络信息安全指数、个人网络信息安全指数三个方面对大数据时代城市网络信息安全状况进行了评估，能够较为客观地反映城市网络信息安全技术的综合水平。因此，选取网络信息安全综合指数来测量网络信息安全技术。

③安全机构设置。网络信息安全机构设置是城市网络信息安全的主要护卫者，网络信息安全机构设置越完善，城市网络信息安全水平越高。换言之，各城市网络信息安全组织机构设置的数量越多，各城市网络信息安全的组织保障越充分。因此，选取各城市网络信息安全机构的数量来测量各市网络信息安全机构设置。数据来源于 2021 年由中国网信官网发布的《全国网络信息安全等级保护测评机构推荐目录》中各城市的网络信息安全机构数量。

④主要领导重视。在中国语境下，领导注意力分配反映了领导对于某项事务及其管理的重视程度[37]。本文通过领导活动中主要领导关于网络信息安全议题的讲话频数来测量领导对网络信息安全的重视程度。领导讲话包括领导主持或参与的会议、调研活动等领导活动中发表的讲话。因此，选取主要领导关于网络信息安全讲话的频数来测量主要领导对网络信息安全的重视程度。数据通过在各城市政府官方网站进行检索整理获得。

⑤安全管理制度。网络信息安全管理制度反映了城市网络信息安全的法治化水平，网络信息安全管理制度越完善，城市网络信息安全法治化水平越高，相应地，城市网络信息安全水平也越高。本文按照标题搜索方式，在“北大法宝网”平台以“网络信息安全”“数据安全”“信息安全”等关键词先初步检索出 36 个城市政府在 2021 年发布的相关法规规章，结合法规规章标题信息，最终确定能反映各城市出台的网络信息安全制度数量。因此，本文通过北大法宝中，各城市出台的网络信息安全制度的频数来测量各城市网络信息安全制度建设水平。

⑥经济条件支持。城市网络信息安全建设水平离不开经济资源的支持，而政府作为城市网络信息安全建设的主体，是经济资源的主要提供者。城市政府的一般公共预算支出水平越高，意味着该城市有更多的财政资源可以投入到城市网络信息安全建设中。因此选取城市政府的一般公共预算支出水平来测量城市网络信息安全建设的经济支持条件。数据来源于 2021 年《中国城市统计年鉴》。

⑦社会需求压力。本文通过各城市的在校大学生人数来测量一个区域的社会需求压力，数据来源于 2021 年各城市统计年鉴。公众受教育程度的高低，影响着公众对网络信息安全风险的认知能力和应对能力，是反映城市网络信息安全社会需求的重要指标。一般而言，受教育程度越高，对网络信息安全的风险感知能力和应对能力也更加敏感，网络信息安全意识越强，由此形成巨大的网络信息安全需求。在校大学生人数在一定程度上代表了一座城市的教育水平与当地民众的受教育程度。因此，选取各城市在校大学生人数来测量社会需求压力。

4.4 变量校准与真值表构建

在用 fsQCA 方法进行分析前，需要对变量进行校准。所谓校准，简单来说，就是将案例中所涉及到的原始变量转化为集合隶属度的过程，是进行必要性与充分性关系分析的前提[38]。首先，本文遵照主流校准方式[39]，将社会需求压力、经济条件支持、网络信息安全人才、网络信息安全技术、网络信息安全机构、主要领导重视等定比变量，选取变量的百分位值，25%（完全不隶属）、50%（交叉点）、75%（完全隶属）作为定性锚点进行校准。其次，对数字城市网络信息安全水平和网络信息安全制度采取直接赋值法进行校准。其中，数字城市网络信息安全水平根据排名进行赋值，排名前 18 赋值为 1，排名后 18 则赋值为 0；网络信息安全制度按照有无网络信息安全制度进行赋值，有赋值为 1，无则赋值为 0。最后，在对每个变量进行校准后，根据变量的赋值规则构建真值表，并利用 fsQCA3.0 软件对真值表进行单个因素的必要性分析和组合条件的充分条件分析，从而得到单个条件变量的必要条件分析结果和组合条件的充分条件分析结果。

5 分析与讨论

定性比较分析包括必要条件分析和充分条件分析两个步骤。必要条件分析是为了测量单个因素对结果变量的解释程度，充分条件分析是为了测量多个因素对结果变量的解释程度。结果用一致性和覆盖度来表示。一致性表示条件变量对结果变量的解释程度，覆盖度表示条件变量可以解释的案例数量[40]。

5.1 单变量分析

进行组态分析之前，需要检验每一个条件变量与结果变量之间的关系，分析

各条件变量是否为网络信息安全水平的必要条件。一般认为，当条件变量的一致性≥0.9，则可以认为该条件变量是结果变量的必要条件[41]。因此，本文使用 fsQCA3.0 软件分析各条件变量的一致性和覆盖度（见表 2）。

表 2　城市高网络信息安全水平的必要条件分析

变量名称	一致性	覆盖度
安全机构设置	0.67	0.71
～安全机构设置	0.33	0.31
主要领导重视	0.63	0.63
～主要领导重视	0.37	0.37
安全管理制度	0.67	0.55
～安全管理制度	0.33	0.43
网络信息安全人才	0.71	0.74
～网络信息安全人才	0.29	0.28
网络信息安全技术	0.68	0.68
～网络信息安全技术	0.32	0.32
经济支持条件	0.78	0.79
～经济支持条件	0.22	0.22
社会需求压力	0.60	0.60
～社会需求压力	0.40	0.40

通过表 2 可以看出，所有条件变量的一致性均小于 0.9，表明这些条件变量都无法单独构成结果变量的必要条件，无法单独对结果变量产生影响[42]。因此，需要考虑条件变量的组合，即进行组态分析，探究多要素对结果变量的共同影响。

5.2　城市高水平网络信息安全建设的充分性分析

本文采用 faQCA3.0 软件分析条件变量的组态模式，在对真值表进行处理的过程中，设定案例数量的域值为 1，同时将一致性阈值设置为 0.75 进行标准化分析，结果如表 3 所示。高网络信息安全水平的影响因素是多元的，共有 5 条条件组态。总的一致性约 0.90，说明符合 5 种组态的城市网络信息安全案例中，90%的城市呈现较高的网络信息安全水平。总覆盖率约 0.48，说明 5 种条件组态可覆盖 48%具有较高网络信息安全水平的城市。从条件组合的影响因素来看，这 5 种生成路径也代表了当前城市高网络信息安全水平的 4 种模式。

表 3　城市高水平网络信息安全建设的组态分析

条件变量	结果变量				
	机构-经济依赖型	制度-环境联动型		领导-经济激励型	机构-人才支持型
	组态 1	组态 2	组态 3	组态 4	组态 5
安全机构设置（SA）	●	⊗	⊗	•	●
主要领导重视（LE）		•	•	●	⊗
安全管理制度（SS）	⊗	●	●		●
网络信息安全人才（SP）	•	•		•	•
网络信息安全技术（ST）	⊗		•	•	•
经济支持条件（PB）	●	●	●	●	•
社会需求压力（EL）	•	●	●	⊗	•
一致性	0.86	0.88	0.90	0.83	0.84
原始覆盖度	0.07	0.12	0.11	0.19	0.11
唯一覆盖度	0.07	0.04	0.03	0.16	0.09
解的一致性	0.48				
解的覆盖度	0.90				

注：●代表核心条件，⊗ 代表核心条件缺失，•代表边缘条件，⊗ 代表边缘条件缺失，空白代表条件不存在。

在 QCA 中，中间解和简约解的关系嵌套可以对结果进行解释，从而识别每个解的核心条件和边缘条件。同时在中间解和简约解中出现的为核心条件，只在中间解中出现的为边缘条件。

5.2.1　机构-经济依赖型

“机构-经济依赖型”对应组态 1，表示为：SA*～SS*EL*SP*PB*～ST，意指即使城市网络信息安全制度建设水平和网络信息安全技术水平不高，在高水平的网络信息安全机构设置和政府的经济条件支持下，以及在较高的社会需求压力和网络信息安全人才队伍建设的辅助下，也能获得较高的网络信息安全水平，而无论主要领导重视程度如何。组态 1 能够解释 7%的案例，并且有 7%的高网络信息安全水平案例能够被这条路径所解释。这一路径的核心条件是网络信息安全机构设置和经济条件支持，代表城市包括郑州市和武汉市。

以武汉市为例。城市网络信息安全建设离不开政府的经济支持和网络信息安全的组织机构保障。在经济支持上，根据《中国城市统计年鉴》，2021 年武汉市公共财政支出约 2407 亿元，在全国 36 个重点城市中位居第 7。大量的财政支出为网络信息安全基础设施建设、人才培养、技术研发等提供了充足的资金保障，为武汉市网络信息安全建设提供了良好的经济支撑。在网络信息安全的组织机构

设置上，根据中国网信官网统计，2021 年武汉市设置了 5 个网络信息安全机构，分别是湖北星野科技发展有限公司、湖北东方网盾信息安全技术有限公司、武汉明嘉信信息安全检测评估有限公司、武汉等保测评有限公司和武汉安域信息安全技术有限公司。这些网络信息安全机构主要负责网络信息安全状况的检测与评估，为武汉市网络信息安全等级测评、安全风险防范等提供了保障。因此，在较完善的组织机构设置和经济条件支持下，武汉市整体网络信息安全建设水平位居全国第 9。

5.2.2 制度-环境联动型

“制度-环境联动型”对应组态 2 和组态 3。组态 2 表示为：～SA*SS*EL*SP*PB*LE，组态 3 表示为：～SA*SS*EL*PB*LE*ST。组态 2 能够解释 12%的案例，有 4%的高网络信息安全水平案例能够被这条路径所解释。组态 3 能够解释 11%的案例，有 3%的高网络信息安全水平案例能够被这条路径所解释。路径 2 和路径 3 核心条件相同，可表示为：～SA*SS*EL*PB*LE。意指当城市当具备较好的网络信息安全制度水平、社会需求压力、经济条件支持时，即使网络信息安全机构设置不够完善，也能获得较高的网络信息安全水平。无论网络信息安全人才队伍建设水平、网络信息安全技术水平如何。代表城市有：南京市、西安市和长沙市。

以长沙市为例。该城市的网络信息安全建设水平，主要受到网络信息安全制度建设和经济条件、社会需求压力等外部环境的影响。在网络信息安全的制度建设上，2021 年 5 月，长沙市发布了《关于长沙市加快网络信息安全产业发展若干政策的补充意见》，强调了网络信息安全对城市网络信息安全的重要价值，提出要“加强城市网络信息安全建设，组建网络信息安全人才培养基地”等目标要求，为长沙市网络信息安全事业发展明确了方向。在网络信息安全的外部环境上，长沙市兼具社会需求压力和经济条件支持的双重环境的影响。一方面，2021 年长沙市在校大学生人数达 69.7 万人。公众受教育程度相对较高，对网络信息安全的感知更加强烈，相应地，对网络信息安全的保障水平也提出了更高的要求，由此推动长沙市不断提升网络信息安全建设水平。另一方面，2021 年长沙市公共财政支出约 1501 亿元，在 36 个重点城市中排名 14，为长沙市网络信息安全建设提供了良好的资金支持。在较好的网络制度建设、社会需求压力和经济支持下，长沙市网络信息安全建设水平处于良好的发展状态中。

5.2.3 领导-经济激励型

“领导-经济激励型”对应组态 4，表示为：SA*～EL*SP*PB*LE*ST。意指在高水平的主要领导重视和经济条件支持下，以及在较高的网络信息安全组织机构设置、网络信息安全人才队伍建设水平、网络信息安全技术水平的辅助下，即使社会需求压力不高，也能获得较高的网络信息安全水平，而无论网络信息安全制度水平如何。组态 4 能够解释 19%的案例，并且 16%的高网络信息安全水平案例能够被这条路径所解释。这一路径的核心条件是主要领导重视和经济支持条件，代表城市有：北京市、天津市和深圳市。

以北京市为例。在主要领导重视上，北京市领导班子非常重视城市网络信息安全建设。例如，2021 年 9 月，北京市市委常委会召开会议，市委书记蔡奇主持会议并发表重要讲话，强调了网络信息安全对当前城市安全的重要影响，提出通过强化关键信息基础设施防护，加强网络信息安全保障能力建设、赋能城市治理和服务群众，推动网络信息安全产业发展等措施来提高网络信息安全的建设水平，为北京市网络信息安全建设提供了行动指南。同时，网络信息安全离不开政府财政资金的保障。根据《中国城市统计年鉴》，2021 年北京市公共财政支出约 7116 亿元，在 36 个重点城市中位居全国第 1，为北京市网络信息安全建设提供了丰富的资金保障。北京市作为国家的政治、经济和文化中心，在经济资源上具有天然的优势，再加上领导对网络信息安全议题的重视，决定了北京市网络信息安全建设在全国的引导性和示范性作用，使得北京市网络信息安全建设水平位居全国首位。

5.2.4 机构-人才支持型

“机构-人才支持型”对应组态 5，表示为：SA*SS*EL*SP*PB*～LE*ST。意指在城市高水平的网络信息安全机构设置和网络信息安全人才队伍建设水平支持下，以及在较高水平的网络信息安全制度建设水平、社会需求压力、经济条件支持和网络信息安全技术的辅助下，即使主要领导重视程度不高，也能获得较高的网络信息安全水平。组态 5 能够解释 11%的案例，并且有 9%的高网络信息安全水平案例能够被这条路径所解释。这一路径的核心条件是网络信息安全机构设置和网络信息安全人才队伍建设水平，代表城市包括成都市和重庆市。

以成都市为例。在网络信息安全机构设置上，根据中国网信官网统计，成都市设置了包括四川省软件和信息系统工程测评中心、成都市锐信安信息安全技术

有限公司等 6 个网络信息安全机构，为成都市提供了良好的网络信息安全组织保障。在网络信息安全人才队伍建设上，2021 年，成都市网络信息安全人才达 26 万人,位居全国第 5。近年来，成都作为全国新一线城市，非常重视网络信息安全人才队伍建设，一方面，成都市通过搭建人才培养平台为成都市“孕育”网络信息安全人才。比如，2021 年 9 月，成都网络信息安全大会将网络信息安全人才吸纳作为大会非常重要的议程，为成都市网络信息安全人才队伍建设搭建平台。另一方面，成都本地高校也非常重视网络信息安全人才的培养，作为国家重点高等院校的电子科技大学，致力于为国家塑造高素质的网络信息安全人才。在较为完善的网络信息安全组织设置和网络信息安全人才队伍建设水平支持下，成都市网络信息安全水平达到全国第 6 的水平。

5.3 城市网络信息安全建设影响因素与组态路径的区域异质性分析

地理位置不同的地区，其技术水平、组织保障和外部环境均有差异，网络信息安全水平的生成路径也有差异。基于此，本文依照我国的地理区分，对东部和中西部地区网络信息安全建设水平的影响因素进行比较研究。

表 4　东、中西部城市网络信息安全水平的组态分析

	东部城市组态			中西部城市组态			
条件变量	领导推动型	制度推动型	领导-经济驱动型	制度-技术驱动型		制度-经济驱动型	
	组态 1	组态 2	组态 3	组态 1	组态 2	组态 3	组态 4
安全机构设置	⨂	⊗	•				
主要领导重视	●	⊗	●	•	•	•	⊗
安全管理制度	•	●		●	●	●	●
网络信息安全人才	•	⊗	•	⊗	⊗	•	•
网络信息安全技术	•	⨂	•	●	●	⊗	•
经济支持条件	•	⨂	●	⊗	•	●	●
社会需求压力	•	⊗	⨂	⊗	•	•	•
一致性	0.87	0.83	0.86	0.90	0.95	0.84	0.97
原始覆盖度	0.13	0.08	0.35	0.12	0.12	0.16	0.21
唯一覆盖度	0.12	0.08	0.34	0.09	0.06	0.10	0.17
解的一致性		0.89			0.91		
解的覆盖度		0.56			0.48		

5.3.1 东部城市网络信息安全建设的组态路径

东部城市：领导推动型、制度推动型和领导-经济驱动型。东部地区的高网

络信息安全水平存在 3 条生成路径，可分别归纳为领导推动型、制度推动型和领导-经济驱动型三种（见表 4）。领导推动型和制度推动型属于组织内部因素驱动的城市网络信息安全建设路径，表明城市如果非常重视网络信息安全的组织建设，可以帮助城市突破技术与环境障碍，从而实现高水平的网络信息安全建设。

领导推动型对应组态 1，该路径受到要领导重视的影响，说明东部地区领导人对网络信息安全的重视，能够有效推动东部地区城市网络信息安全的建设水平。这一路径的代表城市包括北京市、天津市和深圳市。以天津市为例。天津市主要领导人非常重视网络信息安全建设工作。例如，2021 年 5 月 12 日，天津市召开网络信息安全和信息化工作专题会议，市委常委、市委宣传部部长陈浙闽发表重要讲话，提出“提高防范化解网络信息安全领域重大风险的意识和能力、做好关键信息基础设施和信息技术普及应用过程中的防护、筑牢网络信息安全屏障”等措施来提高天津市网络信息安全建设水平，为天津市网络信息安全建设工作明确了方向。主要领导对网络信息安全的高度重视，使得天津市网络信息安全水平位居全国前列。

制度推动型对应组态 2，网络信息安全制度是该路径的核心条件。这一路径表明，在东部城市制度建设能力较强的前提下，即使城市在技术和环境方面建设水平较低，但是城市通过完善网络信息安全法治建设，也能获得较高的网络信息安全水平。这一路径的代表城市是厦门市。2021 年 1 月，厦门市发布了《厦门市公共信用信息归集管理办法》《厦门市守信公共信用信息不公开申请处理管理办法》等网络信息安全政策，明确了公共部门的网络信息安全职责。例如，在《厦门市公共信用信息归集管理办法》第三条中，对公共信息收集提出了明确规定，要求数据归集必须维护国家秘密、商业秘密、个人隐私和其他个人信息的安全。厦门市网络信息安全制度建设，推动厦门市网络信息安全建设水平不断提高。

领导-经济驱动型对应组态 3，该路径受到主要领导重视和经济支持条件的共同影响，表明如果城市具备了较好的主要领导重视和经济支持条件，即使城市网络信息安全技术水平不高，也能获得较高的网络信息安全建设水平。这一路径的代表城市是南京市。为了推动南京市网络信息安全建设，2021 年 12 月 28 日，省委常委、市委书记、市委平安南京建设领导小组组长韩立明主持平安南京建设领导小组会议，学习贯彻习近平总书记对平安中国建设的重要指示精神，将“网

络信息安全”作为平安南京建设的重点任务之一，明确了网络信息安全对城市发展的重要价值。此外，2021 年南京市政府公共财政支出约 1754 亿元，在 36 个城市中排名第 10，为南京市网络信息安全组织建设提供了良好的资金保障。在较高的主要领导重视和经济支持条件下，南京市网络信息安全建设水平位居全国第 8。

通过三条组态结果的分析，可以发现东部地区在较强组织建设能力或者较好组织与环境互动情况下，城市网络信息安全建设会受到较少因素的制约，从而推动城市网络信息安全建设朝着更高水平的方向发展。

5.3.2 中西部城市网络信息安全建设的组态路径

中西部城市：制度-技术驱动型和技术-经济驱动。中西部地区的高网络信息安全水平存在 4 条生成路径，可归纳为制度-技术驱动型和技术-经济驱动型两种类型。组织-技术驱动型对应组态 1 和组态 2，核心条件是网络信息安全制度和网络信息安全技术，表明在中西部城市较高的网络信息安全制度建设水平和网络信息安全技术条件下，即使外部环境因素的支持较低，也能获得较高的网络信息安全水平。这一路径的代表城市是重庆市和贵阳市。以贵阳为例。2021 年 6 月 7 日，贵阳市发布《贵阳市大数据安全管理条例(2021 修正)》，要求“加强大数据安全管理，维护国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进大数据发展应用，推动实施大数据战略”，为贵阳市网络信息安全建设提供了制度保障。在网络信息安全技术方面，贵阳市综合网络信息安全指数 0.698，位居全国第 9。在较好的网络信息安全制度建设水平和网络信息安全技术水平下，贵阳市网络信息安全水平较高。

技术-经济驱动型对应组态 3 和组态 4，核心条件是网络信息安全制度和经济条件支持。表明在城市较高水平的网络信息安全制度建设和政府的公共财政支出水平下，即使组织因素的支持不高，也能获得较高的网络信息安全水平。这一路径的代表城市包括成都市、合肥市、西安市和长沙市。以合肥市为例。在网络信息安全技术水平上，合肥市网络信息安全综合指数为 0.662，在 36 个城市中排名第 11，为合肥市网络信息安全建设的技术研发、技术应用和技术服务等提供了有力的技术支撑。在经济支持上，2021 年合肥市政府公共财政支出约 1164 亿元，为合肥市网络信息安全建设提供了良好的资金支持。在较高的技术水平和经济支持下，合肥市网络信息安全建设水平不断提高。

通过四条组态结果的分析，可以发现中西部地区在制度与技术的互动或者技术与经济的互动条件下，可以获得较高的网络信息安全建设水平，可以作为中西部地区网络信息安全建设水平提升的借鉴之法。

5.4　稳健性检验

在 QCA 研究中，需要对结果的稳健性进行分析，来验证结果的可行性。为了验证分析结果的稳健性，本文遵照主流标准[39]，采用集合论特定的方法（调整一致性阈值）进行稳健性检验。本文将高网络信息安全水平集合的一致性阈值降低 0.05，用 0.7 代替 0.75，再次展开分析，并对调整后的数据进行再次分析，结果如表 5 所示。

表 5　稳健性检验

条件变量	结果变量					
	机构引领型		制度-环境联动型		领导-经济激励型	机构-人才支持型
	组态 1	组态 2	组态 3	组态 4	组态 5	组态 6
安全机构设置	●	●	⊗	⊗	•	●
主要领导重视		⊗	•	•	●	⊗
安全管理制度	⊗	⊗	●	●		•
网络信息安全人才	•	⊗	•		•	●
网络信息安全技术	⊗	⊗		•	•	•
经济支持条件	•	⊗	●	●	●	•
社会需求压力	•	•	●	●	⊗	•
一致性	0.86	0.72	0.88	0.90	0.83	0.84
原始覆盖度	0.07	0.05	0.12	0.11	0.19	0.11
唯一覆盖度	0.06	0.04	0.04	0.03	0.16	0.09
解的一致性	0.89					
解的覆盖度	0.52					

必要条件分析结果显示，单个条件变量仍然无法构成高网络信息安全水平的必要条件；组态分析输出的六种组态中，包括机构引领型、制度-环境联动型、领导-经济激励型、机构-人才支持型，与上述分析结果一致。尽管机构引领型与之前结果机构-经济依赖型有所区别，但通过在组态 1 可以发现，机构-经济依赖型是机构引领型的子集，这是一致性阈值降低的后果。组态的总覆盖率达到 89%，能够解释 52%的高网络信息安全水平案例，与此前相比，覆盖度略有提高。因此，可判断本文的结论是基本稳健的。

6 结语

本文基于 TOE 理论分析框架，通过对 36 个案例进行定性比较分析，总结了高网络信息安全水平的生成路径，得出以下结论：①单个因素不构成高网络信息安全水平的产生的必要条件。通过对单个因素对结果变量的解释程度进行分析，发现网络信息安全水平由多种因素共同影响。尽管单个因素并不能构成高网络信息安全水平的影响因素，但是对高网络信息安全水平的产生具有重要的辅助作用。②技术、组织、环境三个要素之间的联动作用产生了高网络信息安全水平。本文通过对案例进行分析，总结出高网络信息安全水平生成的 4 种模式，即机构-技术依赖型、制度-环境联动型、领导-经济激励型、机构-人才支持型，并着重分析这 4 种模式的生成路径。③东西部城市网络信息安全水平受到不同因素的影响。东部城市可以通过组织内部因素的自我驱动和组织与环境的耦合来获得较高的网络信息安全水平，而中西部城市需要通过组织与技术或组织与环境的耦合来获得较高的网络信息安全水平。

本文通过组态视角分析了影响城市网络信息安全的影响因素以及这些因素间如何发生耦合，在一定程度上突破了既有网络信息安全研究的局限，深化了学界对网络信息安全建设的认识。一是，基于必要条件分析，本文发现单个因素并不是产生高网络信息安全水平的必要条件，说明单个因素并不构成驱动高网络信息安全水平的因素。二是，基于组态化理论，本文系统性探讨了城市网络信息安全的影响因素，并且通过对网络信息安全进行组态分析，揭示了多元化的城市网络信息安全建设路径。三是，本文将城市作为研究对象，对于城市网络信息安全的影响因素识别也更加系统全面，为理解城市网络信息安全水平的影响因素提供了更加科学的理解。四是，通过对东部城市与中西部地区城市网络信息安全建设路径的组态分析，揭示了东部城市与中西部城市差异化的网络信息安全建设路径。

基于研究结论，本文认为当前有效推进我国城市政府网络信息安全建设可以从以下几个方面进行，其一，从网络信息安全的组织来看，需要进一步完善网络信息安全机构的设置，并且要规范这些机构的运行。这需要对已有的网络信息安全机构进行检查，并且对新加入的网络信息安全机构的资质进行严格的审查，防止一些不具备网络信息安全资质的机构给网络信息安全带来威胁。其二，从网络信息安全的技术来看，需要提高网络信息安全技术，弥补技术短板。可以通过与

高校、企业合作，建立起产学研三者并进的网络信息安全技术桥梁。高校作为网络信息安全技术人才的培养池，能够为国家积蓄和培养网络信息安全人才，而企业为网络信息安全人才提供实践场所。因此，政府、企业与高校之间应该相互合作，彼此信任，建立起网络信息安全的防线。其三，从网络信息安全的环境来看，需要加大政府对网络信息安全建设的公共财政投入，无论是网络信息安全机构设置、网络信息安全技术水平的提升，都离不开政府的财政支持。因此，网络信息安全建设需要在资金投入上有所倾向，但也必须防范资金的误用和滥用。最后，因地制宜进行网络信息安全建设。不同地理分区的城市在组织、环境和技术因素方面存在较大差异。因此，各城市应该合理利用相应的资源条件，通过组织、技术与环境之间的联动作用来提高网络信息安全建设水平。

本文也存在一些不足之处有待进一步探索。首先，囿于定性比较分析方法的样本限制，本文主要以 36 座重点城市为例进行了分析，难以覆盖中国所有城市。未来可通过纳入更多的城市样本，采用其他定量方法探究城市网络信息安全建设的影响因素。其次，本文主要从组织、技术与环境三个维度分析了城市网络信息安全的影响因素，尽管与学界主要观点保持一致，但也可能存在其他影响因素有待探索。

参考文献

[1] 周毅. 总体国家安全观视域的网络信息内容治理:进展、内涵与研究逻辑[J].情报理论与实践,2020,43(8):44-50.

[2] 曹惠民，邓婷婷．政府数据治理风险及其消解机制研究[J].电子政务,2021, 217(1):81-91.

[3] 中共中央网络安全和信息化委员会办公室.《中华人民共和国网络信息安全法》[EB/OL].[2016-11-07].http://www.cac.gov.cn/2016-11/07/c_1119867116. htm.

[4] 高凯，邹凯，蒋知义，等. 智慧城市信息安全风险评估指标体系构建[J].现代情报,2022,42(4):110-119.

{5} 范冠峰. 我国网络信息安全法治的困境与对策[J].山东社会科学,2019, 285(5):107-112.

[6] 张志华, 蔡蓉英, 张凌轲. 主要发达国家网络信息安全战略评析与启示[J].现代情报,2017,37(1):172-177.

[7] 蔡蓉英, 张志华, 张凌轲. 基于网络主权的国家竞争情报研究:内涵、动因与机理[J].情报杂志,2016,35(7):13-18

[8] 杨海平. 网络信息安全研究[J].情报科学,2000,(10):944-947

[9] 郭晓苗. 因特网上的信息安全问题[J].情报理论与实践,2000,(2):136-138+135.

[10] Chung K C, Chen C H, Tsai HH, et al.Social media privacy management strategies: A SEM analysis of user privacy behaviours[J].Computer communications,2021, (6):174.

[11] Islam F, Junaid A, Mubashir K M.A bibliometric approach to quantitatively assess current research trends in 5G security[J].Library hi tech,2021,(4):39.

[12] 邓伟志, 范建伟, 施蕾生. 关于建立中国网络社会学的问题[J].江海学刊, 2001, (4):17-24.

[13] 罗文, 乔标, 何颖. 全球新一轮技术创新对中国的影响及对策研究[J].重庆大学学报社会科学版,2014,20(6):46-52.

[14] 张艳丰, 王羽西, 邹凯, 等. 基于模糊的智慧城市信息安全风险要素识别与管理策略研究[J].情报理论与实践,2020,43(10):144-150.

[15] 王以群, 李鹏程, 张力. 网络信息安全中的人因失误分析[J].情报科学,2007, 195(11):1706-1710.

[16] 卢伟, 褚宏启. 教育信息化时代地方高校转型发展的三条路径[J].教育发展研究,2019,39(7):1-6.

[17] 赵志云, 崔海默. 美国网络信息安全新近立法及对我国的启示[J].学术交流, 2017,279(6):136-141.

[18] 肖莹莹. 网络信息安全治理:全球公共产品理论的视角[J].深圳大学学报人文社会科学版,2015,32(1):135-140.

[19] 吉鹏, 许开轶. 政治安全视阈下网络边疆协同治理的困境及其突破路径[J].当代世界与社会主义,2019,140(4):170-177.

[20] 袁正清, 肖莹莹. 网络安全治理的"东盟方式"[J].当代亚太,2016,206(2):80-101-157-158.

[21] Ranjbar A, Maheswaran M.Using Community Structure to Control Information Sharing in Online Social Networks[J].Computer Communications,2014,41(5):11-21

[22] Bernhard D, Lovejoy J P, Ann-Kathrin H, et al.Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences[J].Journal of Computer-mediated Communication,2010,(1):83-108

[23] Fadhil S A, Kadhim L E, Abdurazaq SG.Protection measurements of computer network information security for big data[J].Journal of Discrete Mathematical Sciences and

Cryptography,2021,(7):24.

[24] Ghadge A, Wei? M, Caldwell N D, et al.Managing cyber risk in supply chains: A review and research agenda[J].Supply Chain Management: An International Journal,2020,25(2):223-240.

[25] Kawanaka T, Rokugawa S, Yamashita H.Information Sharing and Security for a Memory Channel Communication Network[J].Industrial Engineering & Management Systems,2018,(17).

[26] Chen J, Miao Y.Research on security evaluation system of network information system based on rough set theory[J].International journal of internet protocol technology,2021,(3):14.

[27] 马晓飞, 艾力彼热 • 艾力肯, 卢奕同. “打上问责补丁” : 网络信息安全问责制的国际实践与对策研究[J].信息资源管理学报,2020,10(6):71-81.

[28] 马民虎, 方婷, 王玥. 美国网络信息安全信息共享机制及对我国的启示[J].情报杂志,2016,35(3):17-23

[29] Tornatzky L G, Fleischer M.The Processes of Technological Innovation[M]. Lexington, MA: Lexington Books,1990:1.

[30] 邱泽奇. 技术与组织: 多学科研究格局与社会学关注[J].社会学研究,2017, 32(4):167-192

[31] 余丽，周旭磊. 技术嵌入：网络空间个体隐私安全体系的建构理路——基于观念、技术与制度的分析框架[J].河南师范大学学报哲学社会科学版,2022, 49(3):52-58

[32] 张志华, 蔡蓉英, 张凌轲. 主要发达国家网络信息安全战略评析与启示[J].现代情报,2017,37(1):172-177.

[33] 陈颀. 网络信息安全、网络战争与国际法——从《塔林手册》切入[J].政治与法律,2014,230(7):147-160.

[34] 卢洪友, 贾莎. 城市公共安全需求影响因素实证研究——对武汉市居民的调查问卷分析[J].经济评论,2011,168(2):102-112.

[35] Ragin C C.The comparative method:Moving beyond qualitative and quantitative methods[M].Berkeley:University of California Press, 1987.

[36] 崔宏桥, 吴焕文. 创业环境如何影响科技人员创业活跃度——基于中国 27 个省市的分析[J].科技进步与对策,2021,38(13):126-134.

[37] 陶鹏，李芳. 灾害管理与政治注意力：框架、进路及方法[J].云南社会科学,2020,234(2):134-140+187-188.

[38] Fiss P C.Building Better Causal Theories; a Fuzzy Set Approach to Typologies in Organization

Research[J].Academy of Management Journal,2011,54(2):393-420.
[39] Ragin C C. Redesigning social inquiry: Fuzzy sets and beyond[M].University of Chicago Press:America,2008.
[40] 郝文强，孟雪. 应急情境下政府开放数据质量的影响因素与组态分析——基于新冠疫情期间省级数据的实证研究[J].情报杂志,2021,40(11):121-128.
[41] 杜运周，刘秋辰，程建青. 什么样的营商环境生态产生城市高创业活跃度？——基于制度组态的分析[J].管理世界,2020,36(9):141-155.
[42] 张明，杜运周. 组织与管理研究中方法的应用：定位、策略和方向[J].管理学报,2019,16(9):1312-1323.

作者贡献声明：
吴钟灿：初稿撰写与论文修改；
郝文强：选题指导与思路建构。

Research on the Influencing Factors and Configuration Paths of Urban Cyber Information Security Construction

——Qualitative comparative analysis of fuzzy sets based on 36 key cities

Wu Zhongcan[1], Hao Wenqiang[2]

[1]School of Management, Minzu University of China, Beijing 100081

[2]School of International Relations & Public Affairs, Fudan University, Shanghai 200433

Abstract: [Purpose/significance]Cyber Information security is critical to personal interests, social stability and national security, and how to improve it has become an urgent issue.[Method/process]Based on TOE theory, this paper uses fuzzy set qualitative comparative analysis to analyze the influencing factors and configuration paths of the cybersecurity construction in China from three aspects: technology, organization, and environment.[Result/conclusion]The result shows that technology, organization and environment are coupled to form four high-level urban cyber security construction paths. They are institutional-economic dependent, system-environment connected, leadership-economic motivated, and institution-talent supported paths. In addition, the cybersecurity construction of cities in different geographic areas shows a differentiated path. Specifically, eastern cities mainly achieve high-level cybersecurity construction through

leadership-driven, institution-promoted, and leadership-economy joint paths, while central and western cities mostly realize high-level cybersecurity construction through institution-technology conjuncted and institution-economy combined paths. Our findings provide multiple path explanations for urban cybersecurity construction and provide insights for promoting urban cyber Information security construction according to local conditions.

Keywords： Urban cyber Information security technology has driven organizational support environmental dependency fuzzy qualitative comparative analysis